Active Directory

Contents

Before You Start

Active Directory is Microsoft's directory and network authentication services architecture. Rumpus includes the ability to authenticate users via Active Directory, and therefore allow access to your Rumpus server based on local user accounts, accounts defined on a network LDAP server.

Administering LDAP and other user account management services is beyond the scope of this article, and it is assumed that you are experienced in managing directory services. For those without an existing Active Directory service, we strongly recommend using the built-in Rumpus user account management database, instead of LDAP. For complete details, see the "Managing User Accounts" article in the "Helpful Info" folder of the Rumpus package.

Active Directory Requirements

The rumpus server needs to be running on a computer that is on the same domain as the Active Directory server. Multi domain environments are not supported.

Because use of a directory server allows for an unlimited number of unique user accounts, Active Directory authentication requires a Rumpus Professional license.

Active Directory Considerations

Because Rumpus uses the Active Directory framework to authenticate users, it is compatible with standard LDAP authentication sources. Again, it is assumed that you are familiar with management of LDAP services.

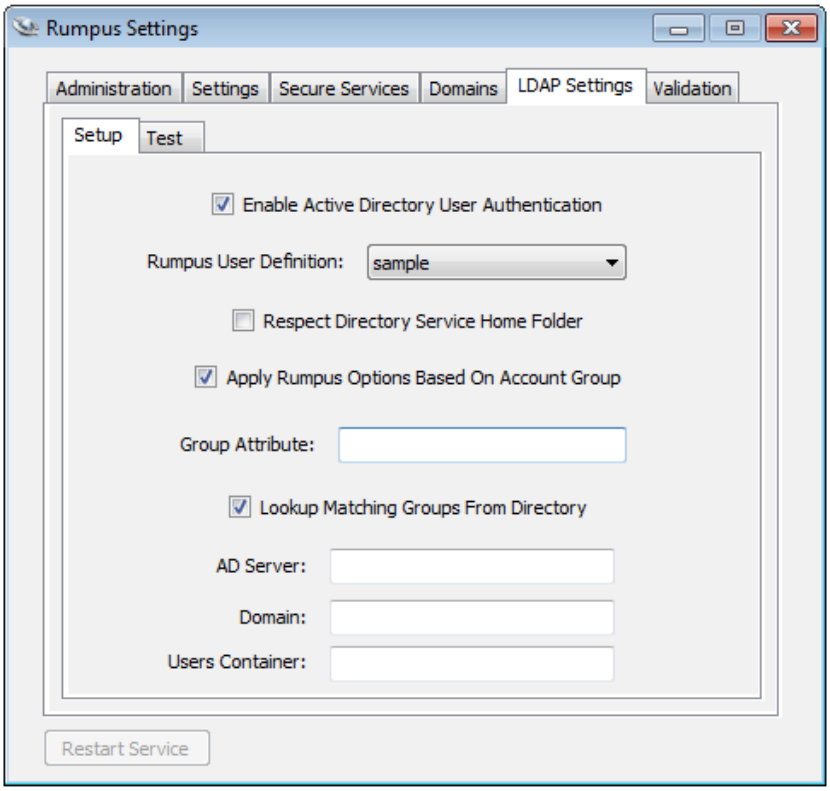
At this point, it is important to understand the difference between "authentication" and "authorization". "Authentication" refers to the act of confirming a user's identity, which in most cases (including all authentication done by Rumpus) means verifying that the user has entered the correct password. "Authorization", on the other hand, defines what the user is permitted to do. Rumpus will authenticate users via any LDAP user account database, but for the most part, authorization (specifying what the LDAP authenticated user is permitted to do) is defined within Rumpus.

So, while users will be authenticated via your Active Directory service, one or more user accounts defined within Rumpus will be applied to all Active Directory authenticated users to define authorization privileges. These accounts will also be used to apply all other user-specific options, such as upload and download notices, account restrictions, and so on.

Configuring Rumpus

At least one Rumpus user account is required to define default privileges for Active Directory authenticated users. To get started, open the "Define Users" window and add a new user to define these privileges. Create the user account as you would any other Rumpus-defined account, and set the password to some suitably difficult to guess password (a long, random string of characters, for example) to ensure that the account is never used directly to access the server. Set the privileges and other account settings as needed to define access rights for default Active Directory authenticated users.

Next, open the “Network Settings” window and flip to the “LDAP Settings” tab, shown below.



The Rumpus “LDAP Settings” tab

Check the “Enable Active Directory User Authentication” checkbox, then select the Rumpus user account which will define Active Directory user access from the “Rumpus User Definition” menu. The user account selected defines the authorization and other user-specific configuration options available in Rumpus. In other words, the privileges, Upload Notice, account restrictions, etc. configured on the Define Users window for the “Rumpus User Definition” user account will be applied by default to all users authenticated via Active Directory.

You will also need to supply the Active Directory server name and domain. The server name should be the full name (for example, “computername.domain.company.com”) or IP address of the Active Directory server. Do not include the Active Directory service port number. The entry for the domain should be the full domain name (as in, “domain.company.com”).

Along with the server and domain, you also have the ability to specify the name of the Users Container that Rumpus should use for account searches. The default is set to “Users”. If you are unsure of the Users Container name to be searched, leave the default in place. If your users are in a differently named container, specify the alternate container name here.

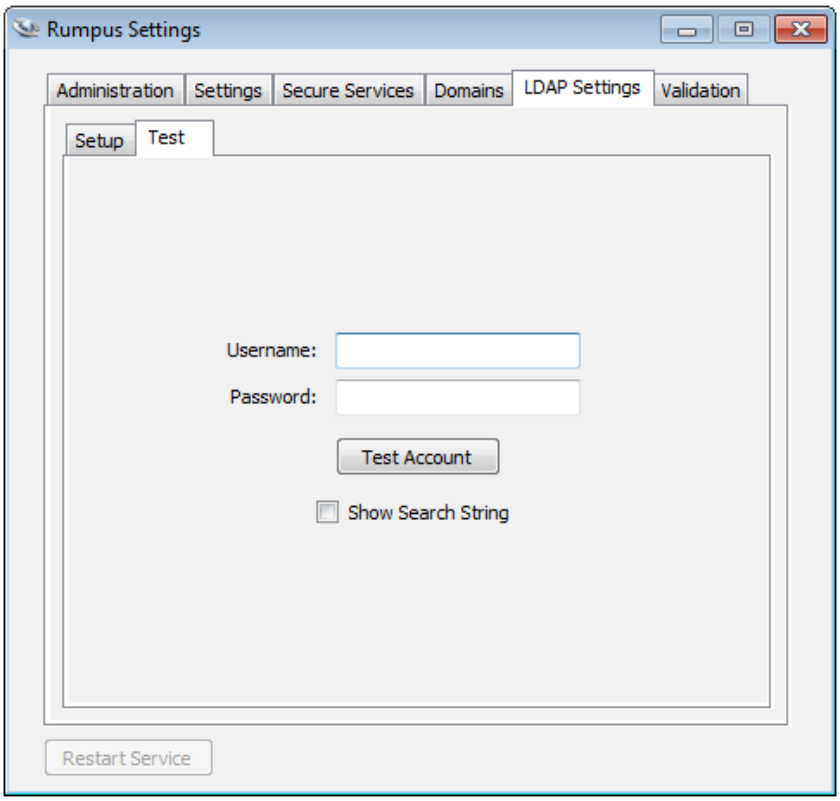
If your user accounts reside in multiple containers, full search syntax can be specified in the Users Container string. The syntax is:

:CN=Users;CN=Accounting

The leading colon (":") in this case tells Rumpus that the Users Container entry isn't simply a container name, but a full search string. To create a full search string, be sure to precede the container names with "CN=" and separate multiple containers with a semi-colon.

Testing Accessible Directory Service Access

To confirm that Rumpus is able to lookup accounts in Active Directory data sources, use the "Test Account" function on the "Test" tab of the LDAP Setup tab. When you supply the name and password of an account in the directory service database, and click "Test Account", Rumpus will query the database and display the user account Home Folder, E-Mail Address and Group.



Testing the ability of Rumpus to access and authenticate users via Active Directory

For details on how the “Group Field” and standard groups list can be applied in Rumpus, see the “Active Directory Groups” section, below.

Enabling the “Show Search String” checkbox will cause each test to display a dialog box that contains the query text sent to the AD server for processing. This option can be used to help in troubleshooting the correct settings for your specific environment.

Specifying Home Folders

While any number of users can be authenticated via Active Directory, chances are each user needs to be granted access only to their own specific home folder. Because Rumpus provides a unique service that is distinct from other network resources, Rumpus does not automatically provide access to any particular folder on the Rumpus server or your file server. There are, however, a number of options that allow you to specify a home folder for users authenticated via LDAP.

When All Users Should Share One Folder

If all users authenticated through Active Directory should be dropped into the same folder, then simply specify that folder for the selected user account in Rumpus. In this case, disable the "Respect Directory Service Home Folder" option, so that the folder chosen in Rumpus will be used as the home folder for all users.

When Each User Should Have A Home Folder On The Rumpus Server

If each authenticated user should be given their own home folder somewhere on the local Rumpus server, then specify a parent folder, followed by a tilde ("~") in the Home Folder field of the selected user account. Also, be sure to disable the "Respect Directory Service Home Folder".

In this configuration, Rumpus will replace the tilde in the home folder path with the user's account name, creating a unique path for each user. When users first log in, the home folder will be created if it doesn't already exist.

For example, if the user accounts "Bob", "Mary" and "Fred" are all authenticated using Active Directory, and the selected Rumpus user account has a home folder of "C:\Rumpus\FTPContent\~", then each of these users will be assigned home folders of:

C:\Rumpus\FTPContent\Bob

C:\Rumpus\FTPContent\Mary

C:\Rumpus\FTPContent\Fred

When Active Directory User Folders Are Correct Paths On The Rumpus Server

In some cases, the Active Directory user folder is a valid path on the Rumpus server and should be used as the user's Rumpus home folder. In this case, simply enable the "Respect Directory Service Home Folder", and set the selected user account home folder to a default path that can be used in case the Active Directory user folder is missing or can't be retrieved.

Active Directory Groups

Groups of users defined in your directory service can be treated differently in Rumpus. To enable this feature, make sure the "Apply Rumpus Options Based On Account Group" checkbox is on.

When the groups feature is enabled, you can set up multiple Rumpus user accounts, each of which will control the access of a specific group of Active Directory authenticated users. For example, users defined in the directory service might be assigned groups of "students" or "teachers". In Rumpus, these groups can be given different privileges and account settings by creating Rumpus user accounts called "students" and "teachers", with those accounts set up accordingly. If an LDAP authenticated user is assigned to a group which does not exactly match the name of a Rumpus user account, the default user definition account will be applied.

There are 2 ways for Rumpus to discover the “Group Name” from your directory service.

Matching Active Directory Groups To Rumpus User Account Names

On the directory server, any user account can be made a member of one or more groups. When a user is authenticated via Active Directory, Rumpus can obtain a list of the groups to which the user is assigned, and compare the list to user account names in the Rumpus user account database. When a match is found, that user account record will be used to determine access privileges for the user. To enable native Active Directory groups support as described here, check the “Lookup Matching Groups From Directory” option on the “Setup” tab of the LDAP Setup tab.

For example, an Active Directory user account might be a member of the groups: admin, everyone, staff and teachers. If any of those group names match an account name defined in Rumpus, the privileges and settings specified for that account will be applied for the user session.

Obtaining The Group Name From A Field In The User Record

When the “Lookup Matching Groups From Directory” option is disabled, Rumpus will not query the directory server for standard groups, but will instead extract the group name from a field in the user record. In this case, whenever Rumpus authenticates a user, it will access the user record field specified by the “Group Attribute”, and use that value to find a matching user account in the Rumpus accounts database.

In Active Directory, fields in the user record are accessed by “attribute”. For example, if you set the Group Attribute to “dsAttrTypeStandard:RealName” and click “Test Account” (with a valid account name and password supplied, of course) you will see the full user account name displayed in the “Group Field” text box.

If you would like to define groups of Active Directory users by specifying a group name in a field of the user account record on the directory server, enter the standard attribute name of that field in the “Group Attribute” field in Rumpus. One common option is to use the “Comments” field associated with user accounts, in which case the Group Attribute in Rumpus would be “dsAttrTypeStandard:Comments”. In this setup, to have a Rumpus user account definition named “BasicUser” applied to select Active Directory authenticated users, you would enter “BasicUser” in the “Comments” field of those user accounts.

Other Uses Of Active Directory Groups

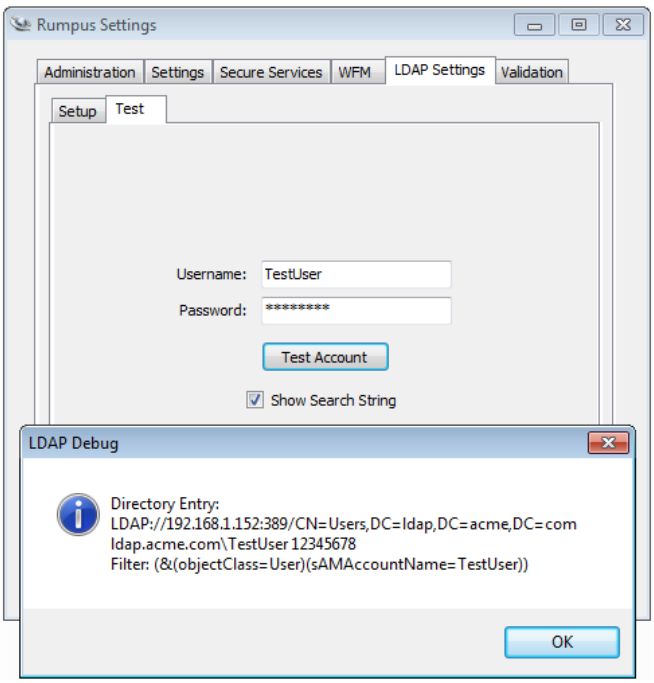
Assume you have a directory service where some user accounts are members of a group called "FTP", and only those users should be permitted to login to your Rumpus server. In this case, first create a user account called "NoAccess", or something similar, with all privileges disabled (including the "Permit Login" privilege). Select that account as the Rumpus User Definition account for Active Directory access. Now, by default, all LDAP authenticated users will be denied access to the server. Next, create a user account called "RumpusFTP" and set the privileges as needed for those users who should be given access. With the "Apply Rumpus Options Based On Account Group" option enabled, Active Directory users with a group name that matches the "RumpusFTP" user account name will be permitted to log in to the server.

The Home Folder for groups of users can also be set in this way. For example, you might have Active Directory users that are assigned groups named "Sales", "Engineering" and "Office", where each group should be granted access to a corresponding content folder on the Rumpus server. Here, you would simply create Rumpus user accounts called "Sales", "Engineering" and "Office", and assign each of those user accounts the appropriate Home Folder.

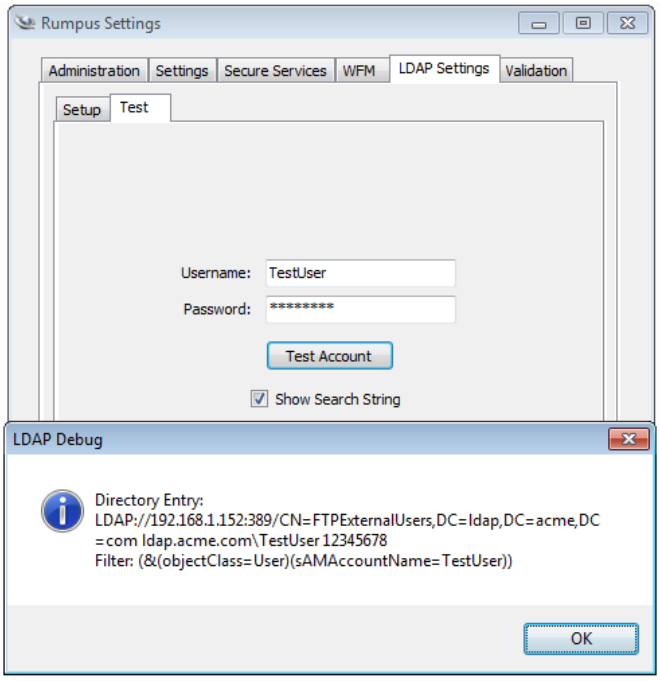
Specifying An Alternate Users Container

When querying the Active Directory service, Rumpus will, by default, search the default “Users" container. You can have Rumpus alter the query to search a different container by entering the name of the container in the Users Container field on the Active Directory setup tab.

For technical administrators familiar with Active Directory queries, the Rumpus AD test function allows you to see the actual test query string generated by Rumpus. Shown below, for example, is the basic query, attempting to authenticate a user in the default “Users” container.

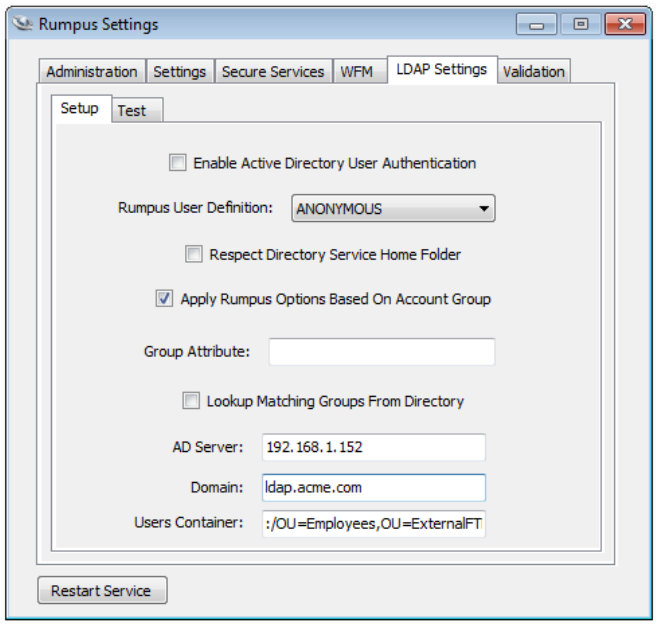


With an alternate Users Container specified ("FTPExternalUsers", in this example), the query becomes:



If necessary, you can even over-ride the Rumpus-generated query with your own. To do this, begin the Users Container entry with a colon (":"), followed by the entire query string. The portion of the Users Container entry following the colon will then be used verbatim as the authentication query.

Rumpus will automatically begin the query with the AD server name and port, but the rest of the query is definable. For example, here is a setup that will generate a query string to search the organizational units "Employees" and "ExternalFTP":



Note the leading slash ("/"), immediately following the colon, that is the necessary delimiter between the server address/port and the query string. Be sure to separate multiple containers with a comma. It is not necessary to add the DC entries for the domain, as they will be added to the search string automatically.

Here is how the resulting query would look: